Early Journal Content on JSTOR, Free to Anyone in the World

This article is one of nearly 500,000 scholarly works digitized and made freely available to everyone in the world by JSTOR.

Known as the Early Journal Content, this set of works include research articles, news, letters, and other writings published in more than 200 of the oldest leading academic journals. The works date from the mid-seventeenth to the early twentieth centuries.

We encourage people to read and share the Early Journal Content openly and to tell others that this resource exists. People may post this content online or redistribute in any way for non-commercial purposes.

Read more about Early Journal Content at http://about.jstor.org/participate-jstor/individuals/early-journal-content.

JSTOR is a digital library of academic journals, books, and primary source objects. JSTOR helps people discover, use, and build upon a wide range of content through a powerful research and teaching platform, and preserves this content for future generations. JSTOR is part of ITHAKA, a not-for-profit organization that also includes Ithaka S+R and Portico. For more information about JSTOR, please contact support@jstor.org.

On Groups whose Orders are Products of Three Prime Factors.

BY F. N. COLE AND J. W. GLOVER.

§1.

INTRODUCTION.

The general problem of the construction of groups of given orders has as yet received comparatively little attention. This is probably due to the fact that the theory of groups has been developed for the most part under the particular phase of the theory of substitutions, in which the operations of a group appear under the form of permutations of letters, and the groups themselves are primarily classified, not according to their order, but according to their degree, i. e. the number of letters affected. Thus we possess a very elaborate series of general theorems limiting the number and character of groups of given degree, while the construction of groups of given orders has thus far been effected only in the most elementary cases. It is, for example, as yet unknown how many and what groups there are of order 24. The foundation for the treatment of groups of given order is, however, already laid in the theory of the composition of groups which, though usually treated as a part of the theory of substitutions, belongs in reality to the pure theory of groups.*

Important and fertile as the consideration of substitution groups is for the theory of equations and of algebraic relations, it is clear that in treating the structure of a group great advantage is gained by discarding all unessential features and regarding the group from its purely formal side, as a group in the abstract, without reference to the content to which its operations may be applied.

In conformity with this idea, Cayley (American Journal, Vols. I and XI) and Kempe (Phil. Trans., Vol. CLXXVII) have determined the groups according to their orders as far as order 12. It is, however, a defect of this method of classification that it proceeds simply according to the order and not the *type* of the groups. Thus, the groups of order pq, where p and q are prime numbers, are all of one of two types, the orders 10, 14, 15, ... presenting no greater complexity than the order 6.

---

* Cf. Sylow's theorems below.

The type of a group depends on the number and mutual relations among the prime factors of its order. Thus the groups of order pq are of only one or of two types according as $p - 1$ is not or is divisible by q. The difficulty of construction naturally increases very rapidly with the number of factors. But if this number does not exceed three, the difficulty is not serious, owing to the easily demonstrated presence of a self-conjugate subgroup in every case.

The groups of prime order are, of course, cyclical. Those of order pq and p^2 are also known.* In the following, those whose order is a product of three, equal or unequal, prime factors are fully determined. These three classes alone comprise 371 of the first 500 orders.

§2.

Sylow's Theorems: The Groups of Order p^2 and pq.

Throughout the following we make constant use of two fundamental theorems of Sylow† which are quite indispensable in the dissection of groups:

I. *A group of order p^α, where p is a prime number, always contains a self-conjugate subgroup of order $p^{\alpha-1}$.*

II. *If the order u of a group is divisible by p^α, but by no higher power of the prime number p, the group contains subgroups of order p^α. These subgroups are all conjugate, and their number is $xp + 1$ where*

$$u = p^\alpha i(xp + 1),$$

i being an integer.

By way of illustration we apply these theorems to the analysis of the groups of order p^2 and pq, where p and q are prime numbers.

I. A group of order p^2 may contain an operation of order p^2. The group is then cyclical, and requires no further consideration. Otherwise its actual operations are all of order p, and the powers of one of these must form a self-conjugate subgroup (Theorem I). Suppose this to be $\{s\} = (1, s, s^2, \dots s^{p-1})$. Any other operation t of the group must transform s into one of its powers; for $\{s\}$ is self-conjugate. Suppose that

---

* Cf. Netto, Theory of Substitutions, pp. 146–9.

† Cf. L. Sylow, Math. Ann. V, pp. 584–94.

$$t^{-1}st = s^{\mu}.$$

Then we have, on repeated transformation by t,

$$t^{-2}st^2 = s^{\mu^2},\ t^{-3}st^3 = s^{\mu^3}, \dots . t^{-p}st^p = s^{\mu^p}.$$

But, as $t^p = 1$, it follows that $t^{-p}st^p = s$. Hence

$$\mu^p \equiv 1 \pmod{p}.$$

This is only possible if $\mu = 1$. Consequently

$$t^{-1}st = s \text{ or } ts = st.$$

The operations s and t are therefore commutative, and accordingly all their combinations can be reduced to the form $s^{\alpha}t^{\beta}$. There are precisely p^2 operations of this form, and these make up the required group. The latter may be written

$$\begin{array}{lllll}
1 & , s & , s^2 & , \dots . s^{p-1} & , \\
t & , st & , s^2t & , \dots . s^{p-1}t & , \\
t^2 & , st^2 & , s^2t^2 & , \dots . s^{p-1}t^2 & , \\
\dots & \dots & \dots & \dots & \\
t^{p-1}, & st^{p-1}, & s^2t^{p-1}, & \dots . s^{p-1}t^{p-1}. &
\end{array}$$

II. Again, a group of order pq may contain an operation of order pq, and is then a cyclical group; otherwise its actual operations are all of orders p or q. By theorem II, there is always one and only one subgroup of order p, which is therefore self-conjugate. Suppose this to be $\{s\} = (1, s, s^2, \dots . s^{p-1})$. Some of the remaining operations are of order q, and any one of these, t, must transform s into one of its powers. Suppose that

$$t^{-1}st = s^{\mu}.$$

Then, as before, we obtain

$$t^{-q}st^q = s^{\mu^q},$$

where, since $t^q = 1$,

$$\mu^q \equiv 1 \pmod{p}.$$

If $p - 1$ is not divisible by q, this congruence has only one root, viz. 1. In this case s and t are commutative, and consequently st is of order pq. The group is then cyclical.

But if q is a divisor of $p - 1$, the above congruence admits of $q - 1$ roots different from 1. If any one of these is μ_1, they may be written

$$\mu_1,\ \mu_1^2,\ \mu_1^3, \dots . \mu_1^{q-1} \pmod{p}.$$

Whichever one of these $q-1$ values of μ is chosen, the resulting group will be the same. For if t transforms s into s^{μ_1}, the successive powers of t will transform s into $s^{\mu_1^2}, s^{\mu_1^3}, \dots.$ And as all the powers of t, except the q^{th}, are of order q, and as every one of them is a power of every other, it is indifferent which one of them is originally taken for t.

Beside the p operations $\{s\}$ the group contains $pq-p$ of order q. These must distribute themselves in p conjugate groups of order q. These groups are transformed in a cycle by the powers of s. In fact, from

$$t^{-\alpha}st^{\alpha} = s^{\mu_1^\alpha}$$

follows

$$s^{-1}t^{\alpha}s = t^{\alpha}s^{1-\mu_1}, \quad s^{-2}t^{\alpha}s^{2} = t^{2\alpha}s^{2(1-\mu_1^\alpha)}, \quad s^{-3}t^{\alpha}s^{3} = t^{3\alpha}s^{3(1-\mu_1^\alpha)}, \dots,$$

where every system $s^{-i}t^{\alpha}s^{i}$ $(\alpha = 0 \dots q-1)$ evidently furnishes a distinct group.

This second type of group of order pq may therefore be written

$$\begin{array}{lllll}
1, & s, & s^2, & \dots & s^{p-1}, \\
t, & ts^{1-\mu_1}, & ts^{2(1-\mu_1)}, & \dots & ts^{(p-1)(1-\mu_1)}, \\
t^2, & t^2s^{1-\mu_1^2}, & t^2s^{2(1-\mu_1^2)}, & \dots & t^2s^{(p-1)(1-\mu_1^2)}, \\
\dots & \dots & \dots & \dots & \dots \\
t^{q-1}, & t^{q-1}s^{1-\mu_1^{q-1}}, & t^{q-1}s^{2(1-\mu_1^{q-1})}, & \dots & t^{q-1}s^{(p-1)(1-\mu_1^{q-1})},
\end{array}$$

or, in a form in which the conjugate relation is accentuated,

$$\begin{array}{lllll}
1, & s, & s^2, & \dots & s^{p-1}, \\
t, & s^{-1}ts, & s^{-2}ts^2, & \dots & s^{-(p-1)}ts^{p-1}, \\
t^2, & s^{-1}t^2s, & s^{-2}t^2s^2, & \dots & s^{-(p-1)}t^2s^{p-1}, \\
\dots & \dots & \dots & \dots & \dots \\
t^{q-1}, & s^{-1}t^{q-1}s, & s^{-2}t^{q-1}s^2, & \dots & s^{-(p-1)}t^{q-1}s^{p-1}.
\end{array}$$

The same results can of course be obtained by the aid of the theory of substitutions,* but the employment of unnecessary apparatus naturally obscures the real process. Moreover, when any group of operations is known, an isomorphic substitution group can be written down at once.† For this purpose we suppose the operations of the group to be numbered in any order. If now we multiply them all by any one among them, s, the resulting products are the same operations again, but in a different order. Corresponding to s, we have therefore a permutation of the numbers designating the several operations. And this permutation evidently affects every number. A similar result holds for any other operation t, and so on. Then, since the original operations form a group, the same is true of the permutations. And these two groups are simply isomorphic. The permutation group, moreover, since all its operations except identity affect every number, is a regular group,* and its degree and order are equal.

---

*Cf. Netto: loc. cit.

† Cayley, Amer. Jour., Vol. I, p. 51.

There is another method by which, given a group of operations, an isomorphic (transitive) substitution group can frequently be found with its degree lower than its order. For example, the not cyclical group of order pq contains p conjugate subgroups of order q. If these are transformed with respect to all the operations in the group, they will simply be permuted among themselves, and these permutations form a group isomorphic with the given one. Moreover, as there is no operation except identity in the group of order pq which, employed as a transformer, leaves all the subgroups of order q unchanged, the group of permutations will also contain pq operations, and the isomorphism is in this case holoedric.

Thus, if in the not cyclical group of order 6,

$$\begin{array}{lll} 1, & s, & s^2, \\ t, & s^{-1}ts, & s^{-2}ts^2, \\ t^2, & s^{-1}t^2s, & s^{-2}t^2s^2, \end{array}$$

the subgroups of order 3, $\{t\}$, $\{s^{-1}ts\}$, $\{s^{-2}ts^2\}$ are numbered 1, 2 and 3, we readily find for the permutations corresponding to s and t,

$$s = (1, 2, 3), \; t = (2, 3),$$

and these generate the required substitution group, which is, of course, the symmetric group of three elements.

In regard to the types of order p^2 and pq, we note further that these can be readily modified so as to furnish groups of higher types. Thus the characteristic feature of the not cyclical group of order pq is that it contains one subgroup of one order and a system of conjugate subgroups of another order, the latter being joined by transformation with respect to the operations of the former. It will at once suggest itself that we may, by way of trial, replace the subgroup of order p by a group of a higher type, for example, p^2, at the same time properly increasing the number of subgroups of order q, or replacing these also by a proper number of groups of a higher type. (Cf. the groups α_2, α_3, β_2, γ_3, γ_4 below.)

---

* Cf. Bolza, Amer. Jour., Vol. XIII, p. 23. It is easily seen that the permutation group above is *transitive*.

§3.

The Groups of Order p^3.

From the first of Sylow's theorems it appears that a group of order p^3 always contains a self-conjugate subgroup of order p^2. We show further that

If a group of order p^3 contains a cyclical subgroup of order p^2, it contains a self-conjugate cyclical subgroup of order p^2.

For suppose that a G_{p^3} contains an operation s of order p^2. If t is any other operation of G_{p^3}, then t^p is contained among the powers of s^p. Otherwise the products $t^\alpha s^\beta$ would furnish at least p^4 different operations.

If now the group $\{s\}$ is not itself self-conjugate, there will be some operation t in the G_{p^3} which transforms $\{s\}$ into p conjugate groups. These groups must have the powers of s^p in common. Beside these they contain $p(p^2-p)$ different operations. There remain, including the powers of s^p, p^2 operations, and as there must always be a self-conjugate subgroup of order p^2, these p^2 operations must constitute this subgroup.

If the latter is cyclical, the theorem is proved. If it is not cyclical, t, which is contained in it, must be of order p and commutative with s^p. The group $\{s^p, t\}$ being self-conjugate, we must then have

$$s^{-1}ts = s^{\alpha p}t^\beta,$$

and $\beta^p \equiv 1 \pmod p$, that is, $\beta = 1$. Then

$$s^{-1}ts = s^{\alpha p}t, \quad \therefore\ tst^{-1} = s^{\alpha p+1},$$

so that t would transform the group $\{s\}$ into itself, which is contrary to assumption.

We may now conveniently divide the groups of order p^3 into two classes, according as they do or do not contain an operation of order p^2.

The former class includes the cyclical group, which, of course, exists for every p. This group, which we designate by α_1, is generated by a single operation s of order p^3. It contains one subgroup of order p, $\{s^{p^2}\}$, and one of order p^2, $\{s^p\}$, and they are both cyclical and both self-conjugate. There are $p-1$ operations of order p, $p(p-1)$ of order p^2, and $p^2(p-1)$ of order p^3.

We proceed now to discuss the not cyclical groups of order p^3.

A.—*An operation of order p^2 present.*

We have shown that there must in this case be a self-conjugate cyclical subgroup of order p^2. Let this be

$$H_{p^2} \equiv \{s\} \equiv (1, s, s^2, \ldots . s^{p^2-1}).$$

If t is any other operation of the group, we have

$$t^{-1}st = s^{\mu},$$

and $\mu^p \equiv 1 \pmod{p}$. Hence $\mu = \kappa p + 1$, and

$$t^{-1}st = s^{\kappa p + 1}.$$

If $\kappa \neq 0$, we have further

$$t^{-2}st^2 = s^{2\kappa p + 1},\ t^{-3}st^3 = s^{3\kappa p + 1}, \ldots .$$

Accordingly, by replacing t by a proper power of t, we can always arrange that $t^{-1}st = s^{p+1}$. There are therefore two distinct types according as

$$t^{-1}st = s \text{ or } t^{-1}st = s^{p+1}.$$

We show further that in each of these types operations of order p occur which are not contained among the powers of s^p. For the identity $t^{-1}st = s^{\kappa p + 1}$ furnishes

$$(t^\lambda s^\nu)^\alpha = t^{\alpha\lambda} s^{\nu\left(\alpha + \frac{\alpha(\alpha-1)}{2}\lambda\kappa p\right)}.$$

If then $\kappa = 0$, or if $p > 2$, we have

$$(t^\lambda s^\nu)^p = t^{p\lambda} s^{p\nu},$$

and since $t^{\lambda p} = s^{\omega p}$, the operation $t^\lambda s^{-\omega}$ will be of order p. The case $p = 2$, $\kappa \neq 0$ is specially considered at a later point.

We may now assume that t is of order p. The equation above then becomes

$$(t^\lambda s^\nu)^p = s^{\nu p\left(1 + \frac{p(p-1)}{2}\lambda\kappa\right)},$$

from which it appears that, since $1 + \dfrac{p(p-1)}{2}\lambda\kappa$ is not divisible by p, all the operations of order p in the group are contained in the not cyclical subgroup $\{t, s^p\}$. The group G_{p^3} therefore contains $p^3 - p^2$ operations of order p^2. These must be distributed in p cyclical groups of order p^2, having the subgroup $\{s^p\}$ in common. Since the group $\{s\}$ is self-conjugate, the remaining $p - 1$ groups are self-conjugate. Their operations of order p^2, together with the p^2 operations $\{t, s^p\}$, make up the entire group.

We now consider the different types separately.

a). The identity is $t^{-1}st = s$, $(t^p = 1)$.

This group α_2 has all its operations commutative, and its subgroups therefore all self-conjugate. The group always exists. It contains

$p + 1$ self-conjugate subgroups of order p, $\{s^p\}$, $\{ts^{\alpha p}\}$, $(\alpha = 0, 1, \ldots . p - 1)$;
1 self-conjugate, not cyclical subgroup of order p^2, $\{s^p, t\}$;
p self-conjugate cyclical subgroups of order p^2, $\{st^\alpha\}$, $(\alpha = 0, 1, \ldots . p - 1)$.

Its operations are distributed according to their orders as follows:

Order......	1	p	p^2
Number....	1	$p^2 - 1$	$p^2(p-1)$

To obtain a corresponding substitution group of order 27 we may take

$s = (1, 2, 3, 4, 5, 6, 7, 8, 9)(10, 11, 12, 13, 14, 15, 16, 17, 18)$
$(19, 20, 21, 22, 23, 24, 25, 26, 27)$,
$t = (1, 10, 19)(2, 11, 20)(3, 12, 21)(4, 13, 22)(5, 14, 23)(6, 15, 24)$
$(7, 16, 25)(8, 17, 26)(9, 18, 27)$.

b). The identity is $t^{-1}st = s^{p+1}$, $(t^p = 1)$.

This type evidently differs from the preceding in that the operation s transforms the p subgroups of order p,

$$\{ts^{\alpha p}\}, \ (\alpha = 0, 1, \ldots . p - 1),$$

in a cycle. It has therefore

1 self-conjugate subgroup of order p, $\{s^p\}$, and
p conjugate subgroups of order p, $\{ts^{\alpha p}\}$, $(\alpha = 0, 1, \ldots . p - 1)$.

Otherwise its subgroups and operations are the same as those of the preceding case.

This group α_3 always exists except when $p = 2$. A substitution group of this type of order 27 is generated by

$$s = (1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9)(10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16,\ 17,\ 18)(19,\ 20,\ 21,\ 22,\ 23,\ 24,\ 25,\ 26,\ 27),$$

$$t = (1,\ 10,\ 19)(2,\ 14,\ 26)(3,\ 18,\ 24)(4,\ 13,\ 22)(5,\ 17,\ 20)(6,\ 12,\ 27)(7,\ 16,\ 25)(8,\ 11,\ 23)(9,\ 15,\ 21).$$

c). *The case* $p = 2$, $\kappa = 1$.

The corresponding group of order 8 may be written

$$\begin{array}{llll} 1, & s, & s^2, & s^3, \\ t, & ts, & ts^2, & ts^3. \end{array}$$

The general identity

$$(t^\lambda s^\nu)^p = t^{\lambda p} s^{\nu\left(p + \frac{p(p-1)}{2}\lambda\kappa p\right)}$$

becomes here

$$(ts^\nu)^2 = t^2 s^{4\nu} = t^2.$$

The operations

$$ts^\nu \quad (\nu = 0,\ 1,\ 2,\ 3)$$

are therefore all of order 2 or all of order 4, according as t is of order 2 or 4.

In the former case

$$t^{-1}st = s^3, \quad (t^2 = 1).$$

There are here five subgroups of order 2,

$$\{s^2\},\ \{t\},\ \{ts\},\ \{ts^2\},\ \{ts^3\},$$

of which the first is self-conjugate, while the first and third and again the second and fourth are conjugate with respect to s. The operation s^2 combined with these subgroups gives rise to two not cyclical groups of order 4, which are self-conjugate. There is also the single cyclical subgroup of order 4, $\{s\}$.

This group is simply the "dihedron" group of order 8. (Cf. Klein, Ikosaeder, Chap. I.) A corresponding substitution group is generated by

$$s = (1,\ 2,\ 3,\ 4)(5,\ 6,\ 7,\ 8),$$
$$t = (1,\ 5)(2,\ 8)(3,\ 7)(4,\ 6).$$

In the second case

$$t^{-1}st = s^3, \quad (t^2 = s^2).$$

Here all the operations are of order 4 except s^2 and 1. There are three self-conjugate cyclical subgroups of order 4, $\{s\}$, $\{ts\}$, $\{t\}$, and one self-conjugate subgroup of order 2, $\{s^2\}$. A corresponding substitution group is generated by

$$s = (1, 2, 3, 4)(5, 6, 7, 8),$$
$$t = (1, 5, 3, 7)(2, 8, 4, 6).$$

B.—*No operation of order p^2 present.*

There must be a self-conjugate not cyclical subgroup of order p^2 present,

$$H_{p^2} \equiv \{s, t\}, \quad (st = ts).$$

Since this group contains $p + 1$ subgroups of order p, any operation u not contained in H_{p^2} must transform one of these groups into itself. If this latter group is $\{s\}$, then

$$u^{-1}su = s.$$

Two cases will then arise according as

$$u^{-1}tu = t, \text{ or } u^{-1}tu = s^{\lambda}t^{\mu}.$$

a). The identities are $t^{-1}st = s$, $u^{-1}su = s$, $u^{-1}tu = t$.

The operations of this group being all commutative, the combination of any two subgroups of order p gives a not cyclical subgroup of order p^2.

The number of subgroups of order p is $\frac{p^3 - 1}{p - 1} = p^2 + p + 1$. These furnish $\frac{(p^2 + p + 1)(p^2 + p)}{2}$ pairs. But as the $p + 1$ subgroups of order p in a group of order p^2 furnish $\frac{(p + 1)p}{2}$ pairs, there are in all

$$\frac{(p^2 + p + 1)(p^2 + p)}{2} \div \frac{(p + 1)p}{2} = p^2 + p + 1$$

not cyclical subgroups of order p^2. All the subgroups of this group are obviously self-conjugate.

This group, which always exists, we denote by α_4. A corresponding substitution group of order 8 is generated by

$$s = (1, 2)(3, 4)(5, 6)(7, 8),$$
$$t = (1, 3)(2, 4)(5, 7)(6, 8),$$
$$u = (1, 5)(2, 6)(3, 7)(4, 8).$$

b). The identities are $t^{-1}st = s$, $u^{-1}su = s$, $u^{-1}tu = s^{\lambda}t^{\mu}$.

We may take s^{λ} as a generator in place of s. Then

$$u^{-1}tu = st^{\mu},$$

where $\mu^{p} \equiv 1 \pmod{p}$. Hence $\mu = 1$, and

$$u^{-1}tu = st.$$

The operation s, being commutative with both t and u, is commutative with all the operations of the group, and in combination with the latter generates $p+1$ not cyclical subgroups of order p^2. These are all the subgroups of this order, for if there were any other, its operations would be commutative with each other and with s, and we should have the preceding type α_4.

Since $\{s, t\}$ and $\{s, u\}$ are self-conjugate, all the subgroups of order p^2 are self-conjugate. Of the subgroups of order p, $\{s\}$ is self-conjugate and the remaining p^2+p divide into $p+1$ sets of p conjugate groups each, the p of each set belonging in the same subgroup of order p^2.

This group α_5 always exists if $p > 2$. If $p = 2$ it does not exist, since from

$$u^{-1}tu = st$$

follows in this case

$$tu = ust, \quad (tu)^2 = tutu = tu\,.\,ust = s,$$

so that tu would be of order $p^2 = 4$. That this does not happen for $p > 2$ appears from the formula

$$(u^{\lambda}t^{\mu}s^{\nu})^{\kappa} = u^{\kappa\lambda}t^{\kappa\mu}s^{\kappa\nu + \lambda\mu\frac{\kappa(\kappa-1)}{2}}.$$

A substitution group of order 27 of this type is generated by

$s = (1, 2, 3)(4, 5, 6)(7, 8, 9)(10, 11, 12)(13, 14, 15)(16, 17, 18)(19, 20, 21)(22, 23, 24)(25, 26, 27)$,

$t = (1, 4, 7)(2, 5, 8)(3, 6, 9)(10, 13, 16)(11, 14, 17)(12, 15, 18)(19, 22, 25)(20, 23, 26)(21, 24, 27)$,

$u = (1, 10, 19)(2, 11, 20)(3, 12, 21)(4, 14, 24)(5, 15, 22)(6, 13, 23)(7, 18, 26)(8, 16, 27)(9, 17, 25)$.

Reviewing the preceding results, we observe that there are always five types of groups of order p^3; that these types are invariable if $p > 2$, but that for $p = 2$ the regular types α_3 and α_5 are missing, while two new exceptional types occur. Also it appears that

In a group of order p^3 every subgroup of order p^2 is self-conjugate.[*]

---

[*] For the general theorem of which this is a particular case cf. Frobenius, Crelle, 101, p. 285.

§4.

The Groups of Order p^2q, $(p > q)$.

From Sylow's theorem follows at once

Every G_{p^2q} contains a single and therefore self-conjugate subgroup of order p^2, and 1, p, or p^2 subgroups of order q.

There are therefore six principal cases to be considered, since the subgroup of order p^2 may be cyclical or not cyclical.

A.—*The G_{p^2} cyclical*; $G_{p^2} = \{s\} = (1, s, s^2, \ldots . s^{p^2-1})$.

a). *A single and therefore self-conjugate subgroup* $H_q = \{t\} = (1, t, t^2, \ldots . t^{q-1})$.

Here
$$s^{-1}ts = t^{\mu},$$
and we must take $\mu = 1$. The operations s and t are commutative, and consequently $\sigma = ts$ is of order p^2q. The G_{p^2q} is therefore cyclical. It contains 1 subgroup of order p^2, 1 of order p, 1 of order q, and 1 of order pq, and these are all cyclical and self-conjugate.

The operations of the group are distributed according to their orders as follows:

Order......	1	q	p	pq	p^2	p^2q
Number....	1	$q-1$	$p-1$	$(p-1)(q-1)$	$p(p-1)$	$p(p-1)(q-1)$

This group β_1 of course always exists.

b). *p conjugate subgroups of order q*; $\dfrac{p-1}{q}$ *an integer.*

Let one of the subgroups of order q be
$$H_q = \{t\} = (1, t, t^2, \ldots . t^{q-1}).$$
Then
$$t^{-1}st = s^{\mu}, \quad \therefore \; s^{-1}ts = ts^{1-\mu}, \quad (\mu^q \equiv 1 \bmod p^2, \; \mu \neq 1).$$
It follows then from
$$t^{-1}s^pt = s^{p\mu}$$
that t and s^p are not commutative. Consequently the powers of s transform $\{t\}$ into p^2 conjugate groups.

The case b), therefore, does not exist.

c). p^2 conjugate subgroups of order q; $\frac{p^2-1}{q}$ an integer.

The p^2 subgroups of order q arise, as we have just seen, by transformation of $\{t\}$ with respect to s. They are

$$\{t\}; \ \{ts^{1-\mu}\}, \ \{ts^{2(1-\mu)}\}, \ldots . \{ts^{(p^2-1)(1-\mu)}\},$$

or, apart from the order of succession,

$$\{t\}, \ \{ts\}, \ \{ts^2\}, \ldots . \{ts^{p^2-1}\}.$$

These groups contain $p^2(q-1)$ operations, which with the p^2 operations $\{s\}$ make up the entire group. As there are no operations of order pq, all the subgroups of this order are of the not cyclical type. They are formed in each case by the combination of the self-conjugate subgroup of order p, $\{s^p\}$ with one of the subgroups of order q. They are

$$\{s^p, ts^\nu\}, \quad (\nu = 0, 1, 2, \ldots . p-1).$$

The subgroups of order q in each of these groups are conjugately connected with respect to the powers of s^p, and the groups themselves are conjugately connected by the remaining powers of s.

This group β_2 is analogous to the not cyclical type of order pq, the group of order p in the latter being here replaced by the cyclical group of order p^2.

The group β_2 exists only if $p-1$ is divisible by q.* Its identity is

$$t^{-1}st = s^\mu, \quad (\mu^q \equiv 1 \bmod p^2, \ \mu \neq 1).$$

It contains

p^2 conjugate subgroups of order q, $\{ts^\nu\}$, $(\nu = 0, 1, \ldots . p^2-1)$;
1 self-conjugate subgroup of order p, $\{s^p\}$;
p conjugate not cyclical subgroups of order pq, $\{s^p, ts^p\}$, $\nu = 0, 1, \ldots . p-1)$;
1 self-conjugate cyclical subgroup of order p^2, $\{s\}$.

Its operations are distributed according to their orders as follows:

Order....	1	q	p	p^2
Number..	1	$p^2(q-1)$	$p-1$	$p(p-1)$

---

* Since there are not cyclical subgroups of order pq.

A substitution group of order 18 of this type is generated by

$$s=(1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9)(10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16,\ 17,\ 18),$$
$$t=(1,\ 10)(2,\ 18)(3,\ 17)(4,\ 16)(5,\ 15)(6,\ 14)(7,\ 13)(8,\ 12)(9,\ 11).$$

B.—*The* G_{p^2} *not cyclical*; $G_{p^2}=\{s,\ t\}$, $(st=ts)$.

a). *A single and therefore self-conjugate subgroup* $H_q\equiv\{u\}\equiv(1,\ u,\ u^2,\ldots u^{q-1})$. In this case we have

$$s^{-1}us=u,\quad t^{-1}ut=u.$$

The operations of the group are, therefore, all commutative. Each of the $p+1$ groups of order p,

$$\{s\},\ \{t\},\ \{ts\},\ \{ts^2\},\ldots.\{ts^{p-1}\},$$

combines with the subgroup $\{u\}$ to form a cyclical subgroup of order pq. These $p+1$ groups, having the group $\{u\}$ in common, contain beside this

$$(p+1)(pq-q)=(p^2-1)q$$

different operations, which with the powers of u make up the entire group.

This group β_3 always exists. Its identities are

$$s^{-1}ts=t,\ s^{-1}us=u,\ t^{-1}ut=u,\ (s^p=t^p=u^q=1).$$

It contains

1 self-conjugate subgroup of order q, $\{u\}$;

$p+1$ self-conjugate subgroups of order p, $\{s\}$, $\{ts^\nu\}$, $(\nu=0,\ 1,\ldots.p-1)$;

$p+1$ self-conjugate cyclical subgroups of order pq,

$$\{u,\ s\},\ \{u,\ ts^\nu\},\ (\nu=0,\ 1,\ldots.p-1);$$

1 self-conjugate not cyclical subgroup of order p^2, $\{s,\ t\}$.

Its operations are distributed according to their orders as follows:

Order....	1	q	p	pq
Number.	1	$q-1$	p^2-1	$(p^2-1)(q-1)$

A substitution group of order 18 of this type is generated by

$$s=(1,\ 2,\ 3)(4,\ 5,\ 6)(7,\ 8,\ 9)(10,\ 11,\ 12)(13,\ 14,\ 15)(16,\ 17,\ 18),$$
$$t=(1,\ 4,\ 7)(2,\ 5,\ 8)(3,\ 6,\ 9)(10,\ 13,\ 16)(11,\ 14,\ 17)(12,\ 15,\ 18),$$
$$u=(1,\ 10)(2,\ 11)(3,\ 12)(4,\ 13)(5,\ 14)(6,\ 15)(7,\ 16)(8,\ 17)(9,\ 18).$$

b). p conjugate subgroups of order q; $\frac{p-1}{q}$ an integer.

Since q is a divisor of $p-1$, any operation u of order q must transform at least two of the $p+1$ subgroups of order p into themselves.* Suppose these to be $\{s\}$ and $\{t\}$. Also either s or t, suppose s, must transform $\{u\}$ into itself; otherwise there would be more than p subgroups of order q. We have therefore the following identities

$$t^{-1}st = s,\ u^{-1}su = s,\ u^{-1}tu = t^{\mu},$$

where $\mu \neq 1$, since $\mu = 1$ leads to the preceding case.

The operations t and u generate a not cyclical subgroup of order pq. This subgroup is evidently self-conjugate, since s is commutative with both t and u. It contains all the operations of order q. The latter being all commutative with s, there are p conjugate cyclical subgroups of order pq. These have the group $\{s\}$ in common, and contain beside this $p(pq-p)$ different operations, which with the p^2 operations $\{s, t\}$ make up the entire group.

The p subgroups of order q are conjugately connected by the operation t. Two of the subgroups of order p, viz. $\{s\}$ and $\{t\}$ are self-conjugate. The remaining $p-1$ subgroups of this order divide into $\frac{p-1}{q}$ sets of q groups conjugately connected by u.

This group β_4 exists only when $p-1$ is divisible by q. Its identities are

$$t^{-1}st = s,\ u^{-1}su = s,\ u^{-1}tu = t^{\mu} \quad (\mu \neq 1),\ (s^p = t^p = u^q = 1).$$

It contains

p conjugate subgroups of order q, $\{t^{-\alpha}ut^{\alpha}\}$, $(\alpha = 0, 1, \ldots . p-1)$;

2 self-conjugate subgroups of order p, $\{s\}$, $\{t\}$;

$\frac{p-1}{q}$ sets of q conjugate subgroups of order p, $\{ts^{\alpha}\}$, $(\alpha = 1, 2, \ldots . p-1)$;

1 self-conjugate not cyclical subgroup of order pq, $\{u, t\}$;

p conjugate cyclical subgroups of order pq, $\{t^{-\alpha}ut^{\alpha}, s\}$, $(\alpha = 0, 1, \ldots . p-1)$;

1 self-conjugate not cyclical subgroup of order p^2, $\{s, t\}$.

Its operations are distributed according to their orders as follows:

Order	1	q	p	pq
Number...	1	$p(q-1)$	p^2-1	$p(p-1)(q-1)$

---

* The case $p = 2$ presents no exception. In this case u might *interchange* $\{t\}$ and $\{s\}$. But then u would leave $\{st\}$ and consequently some other $\{s^{\nu}t\}$ unchanged.

A substitution group of order 18 of this type is generated by

$$s = (1, 2, 3)(4, 5, 6)(7, 8, 9)(10, 11, 12)(13, 14, 15)(16, 17, 18),$$
$$t = (1, 4, 7)(2, 5, 8)(3, 6, 9)(10, 13, 16)(11, 14, 17)(12, 15, 18),$$
$$u = (1, 10)(2, 11)(3, 12)(4, 16)(5, 17)(6, 18)(7, 13)(8, 14)(9, 15).$$

c). p^2 conjugate subgroups of order q; $\frac{p^2-1}{q}$ an integer.

α). $\frac{p-1}{q}$ an integer.

As in the preceding case, every operation u of order q must transform two of the $p+1$ subgroups of order p into themselves. If these are taken for $\{s\}$ and $\{t\}$, we have

$$u^{-1}su = s^{\mu}, \; u^{-1}tu = t^{\nu}.$$

Here μ and ν must both be different from 1; otherwise we should have either β_3 or β_4. The p^2 subgroups of order q are obtained by transforming $\{u\}$ with respect to the p^2 operations $\{s, t\}$.

We have now to distinguish two cases according as μ and ν are equal or unequal.

If $\mu = \nu$, every operation of order q transforms every operation $s^{\alpha}t^{\beta}$ of order p into its μth power. Accordingly, any operation of order p combined with any operation of order q generates a not cyclical subgroup of order pq. There are p of these groups containing s, p containing t, and so on; in all $p(p+1)$. Since $\{s\}$, $\{t\}$, ... are each self-conjugate, these $p(p+1)$ groups divide into $p+1$ sets of p conjugate groups each.

This group β_5 exists only if $p-1$ is divisible by q. It is analogous to the not cyclical type of order pq, the subgroup of order p in the latter being here replaced by the not cyclical subgroup of order p^2. The identities are

$$t^{-1}st = s, \; u^{-1}su = s^{\mu}, \; u^{-1}tu = t^{\mu}, \quad (\mu^q \equiv 1 \bmod p).$$

The group contains

p^2 conjugate subgroups of order q, $\{(t^{\alpha}s^{\beta})^{-1}u\,(t^{\alpha}s^{\beta})\}$, $(\alpha, \beta = 0, 1, \dots. p-1)$;
$p+1$ self-conjugate subgroups of order p, $\{s\}$, $\{ts^{\nu}\}$, $(\nu = 0, 1, \dots. p-1)$;
$p+1$ sets of p conjugate not cyclical subgroups of order pq,
$\{s, u\}$, $\{ts^{\nu}, u\}$, $(\nu = 0, 1, \dots. p-1)$
1 self-conjugate not cyclical subgroup of order p^2, $\{s, t\}$.

The operations are distributed according to their orders as follows:

Order....	1	q	p
Number..	1	$p^2(q-1)$	p^2-1

A substitution group of order 18 of this type is generated by

$s=(1, 2, 3)(4, 5, 6)(7, 8, 9)(10, 11, 12)(13, 14, 15)(16, 17, 18)$,
$t=(1, 4, 7)(2, 5, 8)(3, 6, 9)(10, 13, 16)(11, 14, 17)(12, 15, 18)$,
$u=(1, 10)(2, 12)(3, 11)(4, 16)(5, 18)(6, 17)(7, 13)(8, 15)(9, 14)$.

If $\mu \ddagger \nu$, only $\{s\}$ and $\{t\}$ can be combined with operations u to generate not cyclical subgroups of order pq. Instead of $p(p+1)$ such groups we have here only $2p$, which divide into two sets of p conjugate groups each.

This group β_6 exists only if $p-1$ is divisible by q. The case $q=2$ is inadmissible under this type, since the congruence $\mu^2\equiv 1 \pmod p$ has only one root different from 1. The identities are

$$t^{-1}st=s,\quad u^{-1}su=s^{\mu},\quad u^{-1}tu=t^{\nu},\quad (\mu^q\equiv 1,\ \nu^q\equiv 1 \bmod p,\ \mu \ddagger \nu).$$

The group contains

p^2 conjugate subgroups of order q, $\{(s^{\alpha}t^{\beta})^{-1}u(s^{\alpha}t^{\beta})\}$, $(\alpha, \beta=0, 1, \ldots . p-1)$;
2 self-conjugate subgroups of order p, $\{s\}$, $\{t\}$;
$\frac{p-1}{q}$ sets of q conjugate subgroups of order p, $\{ts^{\nu}\}$ $(\nu=1, 2, \ldots . p-1)$;
2 sets of p conjugate subgroups of order pq, $\{s, u\}$, $\{t, u\}$;
1 self-conjugate not cyclical subgroup of order p^2, $\{s, t\}$.

The operations are distributed according to their orders as in the preceding case.

β). $\frac{p+1}{q}$ *an integer.*

In this case the $p+1$ subgroups of order p divide in respect to transformation by u into $\frac{p+1}{q}$ sets of q groups each. The q groups of any set are either all unchanged by u, or are permuted cyclically. The former assumption would lead to the group β_3, since $p-1$ is not divisible by q. (The case $q=2$ is considered below.) Consequently, to obtain a new type we must assume that u transforms any subgroup of order p, as $\{s\}$, into a different subgroup of order p, as $\{t\}$,

$$u^{-1}su = t.$$

Also, the order of u being $q > 2$, we must take

$$u^{-2}su^2 = u^{-1}tu = s^{\lambda}t^{\mu}, \quad (\lambda \neq 0,\ \mu \neq 0),$$

where λ and μ must be so chosen that

$$u^{-q}su^q = u^{-(q-2)}(s^{\lambda}t^{\mu})\,u^{q-2} = s.$$

As no subgroup of order p is transformed into itself by any operation of order q, there is no self-conjugate subgroup of order p, and for the same reason, no subgroup of order pq.

This group β_7 exists only if $p+1$ is divisible by q. Also the case $q = 2$ is inadmissible, since we must then have

$$u^{-1}su = t,\ u^{-1}tu = s,$$

and therefore

$$u^{-1}(st)\,u = st,$$

so that u would transform one and therefore two groups of order p into themselves, and we should have β_3 or β_4. The group has only two generators connected by the identity

$$(u^{-1}su)^{-1}s\,(u^{-1}su) = s \text{ or } u^{-1}s^{-1}usu^{-1}su = s.$$

The group contains

p^2 conjugate subgroups of order q, $(s^{\alpha}t^{\beta})^{-1}u\,(s^{\alpha}t^{\beta})$, $(\alpha,\ \beta = 0,\ 1, \ldots . p-1)$;

$\dfrac{p+1}{q}$ sets of q conjugate subgroups of order p; no subgroup of order pq;

1 self-conjugate subgroup of order p^2, $\{s,\ t\}$.

Its operations are of the same orders as in the two preceding cases.

The lowest order for this type is $5^2 . 3 = 75$. A substitution group of this type and order is generated by

$s =$ (1, 2, 3, 4, 5) (6, 7, 8, 9, 10) (11, 12, 13, 14, 15)(16, 17, 18, 19, 20)
(21, 22, 23, 24, 25)(26, 27, 28, 29, 30)(31, 32, 33, 34, 35)(36, 37, 38, 39, 40)
(41, 42, 43, 44, 45)(46, 47, 48, 49, 50)(51, 52, 53, 54, 55)(56, 57, 58, 59, 60)
(61, 62, 63, 64, 65)(66, 67, 68, 69, 70)(71, 72, 73, 74, 75),

$u =$ (1, 26, 51)(2, 31, 75)(3, 36, 69)(4, 41, 63)(5, 46, 57)(6, 50, 52)(7, 30, 71)
(8, 35, 70)(9, 40, 64)(10, 45, 58)(11, 44, 53)(12, 49, 72)(13, 29, 66)(14, 34, 65)
(15, 39, 59)(16, 38, 54)(17, 43, 73)(18, 48, 67)(19, 28, 61)(20, 33, 60)
(21, 32, 55)(22, 37, 74)(23, 42, 68)(24, 47, 62)(25, 27, 56).

§5.

The Groups of Order pq^2, $p > q$.

The application of Sylow's theorem shows that

Every group of order pq^2, *the case* $p=3$, $q=2$ *excepted, contains a single and therefore self-conjugate subgroup of order* p, *and in every case either* 1 *or* p *subgroups of order* q^2.

The self-conjugate subgroup of order p we designate throughout by

$$H_p \equiv \{s\} \equiv (1, s, s^2, \ldots . s^{p-1}).$$

The subgroups of order q^2 being either cyclical or not cyclical, there are four general cases to be discussed.

A.—*A single and therefore self-conjugate* H_{q^2}.

a). *The* H_{q^2} *cyclical*; $H_{q^2} \equiv \{t\} \equiv (1, t, t^2, \ldots . t^{q^2-1})$.

The group $\{t\}$ being self-conjugate, we have

$$s^{-1}ts = t^{\mu}, \quad (\mu^p \equiv 1 \bmod q^2, \ \therefore \ \mu = 1).$$

Accordingly, s and t being commutative, st is of order pq^2, and the group is cyclical.

This group γ_1 contains 1 self-conjugate cyclical subgroup of each of the orders q, p, pq, q^2. Its operations are distributed according to their orders as follows:

Order …	1	q	p	pq	q^2	pq^2
Number . .	1	$q-1$	$p-1$	$(p-1)(q-1)$	$q(q-1)$	$(p-1)(q-1)q$

b). *The* H_{q^2} *not cyclical*; $H_{q^2} \equiv \{t, u\}$, $(tu = ut)$.

Since $\{s\}$ is self-conjugate, we must have

$$t^{-1}st = s^{\mu}, \qquad u^{-1}su = s^{\nu},$$

$$\therefore \ s^{-1}ts = ts^{1-\mu}, \quad s^{-1}us = us^{1-\nu}.$$

But, as $\{t, u\}$ is also self-conjugate, it follows that $\mu = \nu = 1$. The identities are therefore

$$t^{-1}st = s, \quad u^{-1}su = s, \quad t^{-1}ut = u,$$

and the operations of the group are all commutative.

The operation s in combination with the operations t, u, tu, tu^2, ... tu^{q-1} generates $q + 1$ cyclical groups of order pq. These groups having the power of s in common, contain beside these $(q + 1)p(q - 1) = p(q^2 - 1)$ different operations, which with the powers of s make up the entire group.

This group γ_2 contains

$q + 1$ self-conjugate subgroups of order q, $\{t\}$, $\{ut^a\}$, $(a = 0, 1, \dots q - 1)$;
1 self-conjugate subgroup of order p, $\{s\}$;
$q + 1$ self-conjugate cyclical subgroups of order pq, $\{s, t\}$, $\{s, ut^a\}$, $(a = 0, 1, \dots q - 1)$;
1 self-conjugate not cyclical subgroup of order q^2, $\{u, t\}$.

The operations are distributed according to their orders as follows:

Order....	1	q	p	pq
Number..	1	$q^2 - 1$	$p - 1$	$(p - 1)(q^2 - 1)$

A substitution group of order 12 of this type is generated by

$$s = (1, 2, 3)(4, 5, 6)(7, 8, 9)(10, 11, 12),$$
$$t = (1, 4)(2, 5)(3, 6)(7, 10)(8, 11)(9, 12),$$
$$u = (1, 7)(2, 8)(3, 9)(4, 10)(5, 11)(6, 12).$$

B.—*p conjugate H_{q^2}'s; $\frac{p-1}{q}$ an integer.*

a). The H_{q^2}'s cyclical.

Denoting any one of the H_{q^2}'s by $\{t\}$, we must have

$$t^{-1}st = s^\mu, \quad (\mu^{q^2} \equiv 1 \bmod p).$$

Here $\mu \not\equiv 1$, for $\mu = 1$ would lead to the group γ_1. The p H_{q^2}'s are therefore obtained by transforming $\{t\}$ with respect to s. They are, apart from their order of sequence,

$$\{t\}, \{ts\}, \{ts^2\}, \dots \{ts^{p-1}\}.$$

There are now two cases to be distinguished, according as μ is a primitive root of the congruence $\mu^q \equiv 1 \pmod{p}$, or of the congruence $\mu^{q^2} \equiv 1 \pmod{p}$.

In the former case t^q is commutative with s. The powers of t^q are common to all the H_{q^2}'s. These powers combined with s generate a self-conjugate cyclical subgroup of order pq. The pq operations of the latter and the $p(q^2-q)$ operations of order q^2 in the H_{q^2}'s make up the entire group.

This group γ_3 exists only when $\frac{p-1}{q}$ is an integer. Its identity is

$$t^{-1}st = s^{\mu}, \quad (\mu^q \equiv 1 \bmod p).$$

It contains

1 self-conjugate subgroup of order q, $\{t^q\}$;
1 self-conjugate subgroup of order p, $\{s\}$;
1 self-conjugate cyclical subgroup of order pq, $\{s, t^q\}$;
p conjugate cyclical subgroups of order q^2, $\{s^{-\alpha}ts^{\alpha}\}$, $(\alpha = 0, 1, \ldots . p-1)$.

Its operations are distributed according to their orders as follows:

Order....	1	q	p	pq	q^2
Number..	1	$q-1$	$p-1$	$(p-1)(q-1)$	$pq(q-1)$

A substitution group of order 12 of this type is generated by

$$s = (1, 2, 3)(4, 5, 6)(7, 8, 9)(10, 11, 12),$$
$$t = (1, 4, 7, 10)(2, 6, 8, 12)(3, 5, 9, 11).$$

In the second case, μ is a primitive root of the congruence $\mu^{q^2} \equiv 1 \pmod{p}$. In this case the H_{q^2}'s differ in all their operations except identity. Their operations of order q combine with s to generate a not cyclical group of order pq.

This group γ_4 exists only if $\frac{p-1}{q^2}$ is an integer. Its identity is

$$t^{-1}st = s^{\mu}, \quad (\mu^{q^2} \equiv 1 \bmod p, \ \mu^q \not\equiv 1 \bmod p).$$

The group contains

p conjugate subgroups of order q, $\{s^{-\alpha}t^q s^{\alpha}\}$, $(\alpha = 0, 1, \ldots . p-1)$;
1 self-conjugate subgroup of order p, $\{s\}$;
1 self-conjugate not cyclical subgroup of order pq, $\{s, t^q\}$;
p conjugate cyclical subgroups of order q^2, $\{s^{-\alpha}ts^{\alpha}\}$, $(\alpha = 0, 1, \ldots . p-1)$.

Its operations are distributed according to their orders as follows:

Order....	1	q	p	q^2
Number..	1	$p(q-1)$	$p-1$	$pq(q-1)$

A substitution group of order 20 of this type is generated by

$$s = (1, 2, 3, 4, 5)(6, 7, 8, 9, 10)(11, 12, 13, 14, 15)(16, 17, 18, 19, 20),$$
$$t = (1, 6, 11, 16)(2, 8, 15, 19)(3, 10, 14, 17)(4, 7, 13, 20)(5, 9, 12, 18).$$

The groups γ_3 and γ_4 are analogous to the not cyclical type of order pq, the groups of order q in the latter being here replaced by the cyclical groups of order q^2.

b). *The H_{q^2}'s not cyclical.*

Any one of the H_{q^2}'s being denoted by $\{t, u\}$, we have

$$t^{-1}st = s^{\mu}, \quad u^{-1}su = s^{\nu}.$$

Here μ and ν cannot both be equal to 1, for this would give the group γ_2. We have two cases to consider, according as one or both of them is different from 1.

In the first case, suppose $\mu = 1$, $\nu \neq 1$. Then

$$t^{-1}st = s, \quad u^{-1}su = s^{\nu};$$
$$\therefore \; s^{-1}ts = t, \quad s^{-1}us = us^{1-\nu}.$$

The p H_{q^2}'s arise by transformation of $\{t, u\}$ with respect to s. These p groups, having the subgroup $\{t\}$ in common, contain beside this $p(q^2 - q)$ different operations. The combination of s with t furnishes a cyclical group of order pq, the pq operations of which complete the entire group.

This group γ_5 exists only if $\dfrac{p-1}{q}$ is an integer. Its identities are

$$t^{-1}ut = u, \quad t^{-1}st = s, \quad u^{-1}su = s^{\nu}, \quad (\nu \neq 1).$$

The group contains

1 self-conjugate subgroup of order q, $\{t\}$;
q sets of p conjugate subgroups of order q;
$\{s^{-\alpha}(ut^{\beta})s^{\alpha}\}$, $(\alpha = 0, 1, \ldots . p-1, \; \beta = 1, 2, \ldots . q-1)$;
1 self-conjugate subgroup of order p, $\{s\}$;

1 self-conjugate cyclical subgroup of order pq, $\{s, t\}$;
p conjugate not cyclical subgroups of order q^2, $\{t, s^{-\alpha}us^{\alpha}\}$, $(\alpha = 0, 1, \dots . p-1)$.

The operations are distributed according to their orders as follows:

Order....	1	q	p	pq
Number..	1	$(pq+1)(q-1)$	$p-1$	$(p-1)(q-1)$

A substitution group of order 12 of this type is generated by

$$s = (1, 2, 3)(4, 5, 6)(7, 8, 9)(10, 11, 12),$$
$$t = (1, 4)(2, 5)(3, 6)(7, 10)(8, 11)(9, 12),$$
$$u = (1, 7)(2, 9)(3, 8)(4, 10)(5, 12)(6, 11).$$

Secondly, suppose that in the identities

$$t^{-1}st = s^{\mu}, \quad u^{-1}su = s^{\nu},$$

neither μ nor ν is equal to 1. If $\mu = \nu$, we have

$$(u^{-1}t)^{-1}s\,(u^{-1}t) = s,$$

which leads to the group γ_5. Accordingly we must take

$$t^{-1}st = s^{\mu}, \qquad u^{-1}su = s^{\nu}, \qquad (\mu \ddagger 1, \ \nu \ddagger 1, \ \mu \ddagger \nu);$$
$$\therefore \ s^{-1}ts = ts^{1-\mu}, \quad s^{-1}us = us^{1-\nu}.$$

As before, the $p\,H_{q^2}$'s arise by transformation of $\{t, u\}$ by s. These groups have now no operation except identity common to any two of them. Their $p\,(q^2-1)$ operations of order q with the p operations $\{s\}$ make up the entire group.

This group γ_6 exists only if $\frac{p-1}{q}$ is an integer. Also q must be > 2, for the congruence $\mu^2 \equiv 1 \pmod{p}$ has only one root different from 1. The identities are

$$u^{-1}tu = t, \ t^{-1}st = s^{\mu}, \ u^{-1}su = s^{\nu}, \ (\mu \ddagger 1, \ \nu \ddagger 1, \ \mu \ddagger \nu).$$

The group contains

$q+1$ sets of p conjugate subgroups of order q,
$\{s^{-\alpha}ts^{\alpha}\}$, $\{s^{-\alpha}(t^{\beta}u)s^{\alpha}\}$, $(\alpha = 0, 1, \dots . p-1; \ \beta = 0, 1, \dots . q-1)$;
1 self-conjugate subgroup of order p, $\{s\}$;
p conjugate not cyclical subgroups of order q^2, $s^{-\alpha}\{t, u\}s^{\alpha}$, $(\alpha = 0, 1, \dots . p-1)$.

The operations are distributed according to their orders as follows:

Order....	1	q	p
Number..	1	$p(q^2-1)$	$p-1$

A substitution group of order 63 of this type is generated by

$s =$ (1, 2, 3, 4, 5, 6, 7)(8, 9, 10, 11, 12, 13, 14)(15, 16, 17, 18, 19, 20, 21)
(22, 23, 24, 25, 26, 27, 28)(29, 30, 31, 32, 33, 34, 35)(36, 37, 38, 39, 40, 41, 42)
(43, 44, 45, 46, 47, 48, 49)(50, 51, 52, 53, 54, 55, 56)(57, 58, 59, 60, 61, 62, 63).
$t =$ (1, 8, 15)(2, 10, 19)(3, 12, 16)(4, 14, 20)(5, 9, 17)(6, 11, 21)(7, 13, 18)
(22, 29, 36)(23, 31, 40)(24, 33, 37)(25, 35, 41)(26, 30, 38)(27, 32, 42)(28, 34, 39)
(43, 50, 57)(44, 52, 61)(45, 54, 58)(46, 56, 62)(47, 51, 59)(48, 53, 63)(49, 55, 60).
$u =$ (1, 22, 43)(2, 26, 45)(3, 23, 47)(4, 27, 49)(5, 24, 44)(6, 28, 46)(7, 25, 48)
(8, 29, 50)(9, 33, 52)(10, 30, 54)(11, 34, 56)(12, 31, 51)(13, 35, 53)(14, 32, 55)
(15, 36, 57)(16, 40, 59)(17, 37, 61)(18, 41, 63)(19, 38, 58)(20, 42, 60)(21, 39, 62).

This group and the preceding are again analogous to the not cyclical type of order pq, the subgroups of order q in the latter being here replaced by the not cyclical subgroups of order p^2.

C.—*The special group of order* 12.

For the order 12, Sylow's theorem shows the possibility of an exceptional group with *four* conjugate subgroups of order 3. These four subgroups contain 8 operations of order 3. The 4 remaining operations must then form a self-conjugate subgroup of order 4.

The latter cannot be cyclical; for if we denote it by

$$1,\ t,\ t^2,\ t^3$$

and any operation of order 3 by s, we should have

$$s^{-1}ts = t\,, \quad (\alpha^3 \equiv 1 \bmod 4)\,.$$

Then $\alpha = 1$, and st would be of order 12, so that the G_{12} would be cyclical.

The exceptional group of order 12 therefore contains 8 operations of order 3, 3 of order 2, and identity. If we denote the operations of order 2 by t, u,

ut, and any operation of order 3 by s, then s transforms t, u, ut in a cycle. For if s left t unchanged, st would be of order 6. Accordingly we have the identities

$$u^{-1}tu = t, \quad s^{-1}ts = u, \quad s^{-1}us = ut,$$

from which the group is fully determined.

This group is in fact isomorphic with the alternating group of 4 letters.

§ 6.

The Groups of Order pqr; $(p > q > r)$.

From Sylow's theorem a group G of order pqr contains either 1 or qr subgroups of order p.

In the latter case these qr subgroups would contain $qr(p-1)$ distinct operations of order p, leaving only qr operations of G to be determined. Among these qr operations there must be at least one, t, of order q, and at least one, u, of order r. If t transforms u into itself, then t and u generate a cyclical group of order qr, which exactly supplies the qr missing operations. This group contains only a single subgroup, $\{t\}$, of order q, which is therefore the only subgroup of this order contained in G. Again, if t does not transform u into itself, then it transforms the group $\{u\}$ into q conjugate groups of order r. These contain $q(r-1)$ distinct operations of order r, leaving only the q powers of t. In this case also, then, the group G contains only one subgroup, $\{t\}$, of order q.

Now, if s is any operation of order p contained in G, then s must transform t into itself. Accordingly, s and t generate a cyclical group H of order pq. This group contains all the operations of order p, q or pq which occur in G. For if τ is any such operation, contained in G but not in H, then the operations

$$H, \ \tau H, \tau^2 H, \ldots . \tau^{q-1} H$$

will all be different. But their number is $pq^2 > pqr$. But H contains only one subgroup $\{s\}$ of order p, which is therefore the only subgroup of order p contained in G.

Accordingly, a group of order pqr contains only one subgroup of order p.

If the subgroup of order p is $\{s\}$, and if t is any operation of order q contained in G, then t must transform s into one of its powers. Consequently, s and t generate a group of order pq. By the same reasoning employed above, this group contains all the operations of order p, q, or pq that occur in G; it is therefore self-conjugate.

Every group G of order pqr contains a self-conjugate subgroup H of order pq. The latter contains all the operations of order p, q, or pq that occur in the entire group.

We have now to distinguish two principal cases according as the subgroup H of order pq is cyclical or not cyclical. Throughout we use s, t, and u, as heretofore, to designate operations of orders p, q, and r.

A.—*The subgroup H cyclical*; $st = ts$.

This case can occur for all values of p and q, and is the only possibility if q is not a divisor of $p-1$.

Since G contains here only one subgroup of order q, as well as only one of order p, we must have

$$u^{-1}su = s^{\mu}, \quad u^{-1}tu = t^{\nu}.$$

There are four subcases, according as

$$1)\ \mu = 1, \nu = 1; \quad 2)\ \mu = 1, \nu \neq 1; \quad 3)\ \mu \neq 1, \nu = 1; \quad 4)\ \mu \neq 1, \nu \neq 1.$$

1) In this case, s, t and u being all commutative, the operation stu is of order pqr, and G is cyclical. This group, δ_1, contains one subgroup of each of the orders p, q, r, pq, pr, and qr; and these subgroups are all cyclical and self-conjugate. The operations of δ_1 are distributed according to their orders as follows:

Order...	1	p	q	r	pq	pr	qr	pqr
Number.	1	$p-1$	$q-1$	$r-1$	$(p-1)(q-1)$	$(p-1)(r-1)$	$(q-1)(r-1)$	$(p-1)(q-1)(r-1)$

2). This case requires that r should be a divisor of $p-1$. The operations u and t generate a not cyclical group of order qr, in which the q subgroups of order r are

$$\{t^{-a}ut^{a}\}, \quad (\alpha = 0, 1, \ldots . q-1).$$

The operations $t^{-a}ut^{a}$ are all commutative with s. Each of them, taken with s, generates a cyclical group of order pr. These q groups have only the powers of s in common; beside these they contain $q(pr-p)$ distinct operations, which with the operations of H make up the entire group.

This group δ_2 exists only if r is a divisor of $p-1$. Its identities are $st=ts$, $su=us$, $u^{-1}tu=t^{\mu}$. It contains

1 self-conjugate subgroup of order p, $\{s\}$;
1 self-conjugate subgroup of order q, $\{t\}$;
q conjugate subgroups of order r, $\{t^{-a}ut^{a}\}$, $(\alpha=0, 1, \ldots . q-1)$;
1 self-conjugate cyclical subgroup of order pq, $\{s, t\}$;
1 self-conjugate not cyclical subgroup of order qr, $\{t, u\}$;
q conjugate cyclical subgroups of order pr, $\{s, t^{-a}ut^{a}\}$.

The operations of the group are distributed according to their orders as follows:

Order ..	1	p	q	r	pq	pr
Number.	1	$p-1$	$q-1$	$q(r-1)$	$(p-1)(q-1)$	$q(p-1)(r-1)$

A substitution group of this type of order 30 is generated by

$s=(1, 2, 3, 4, 5)(6, 7, 8, 9, 10)(11, 12, 13, 14, 15)$
$(16, 17, 18, 19, 20)(21, 22, 23, 24, 25)(26, 27, 28, 29, 30)$.
$t=(1, 6, 11)(2, 7, 12)(3, 8, 13)(4, 9, 14)(5, 10, 15)$
$(16, 21, 26)(17, 22, 27)(18, 23, 28)(19, 24, 29)(20, 25, 30)$.
$u=(1, 16)(2, 17)(3, 18)(4, 19)(5, 20)$
$(6, 26)(7, 27)(8, 28)(9, 29)(10, 30)$
$(11, 21)(12, 22)(13, 23)(14, 24)(15, 25)$.

3). This case differs from 2) only in the exchange of the roles of s and t.

4). In this case r must be a divisor of both $p-1$ and $q-1$. The operations of the group can then be written as follows (where $\sigma=st$):

$$\begin{array}{lllll}
1 & , \sigma & , \sigma^2 & , \ldots . \sigma^{pq-1} & , \\
u & , \sigma^{-1}u\sigma & , \sigma^{-2}u\sigma^2 & , \ldots . \sigma u\sigma^{-1} & , \\
u^2 & , \sigma^{-1}u^2\sigma & , \sigma^{-2}u^2\sigma^2 & , \ldots . \sigma u^2\sigma^{-1} & , \\
\ldots\ldots & \ldots\ldots & \ldots\ldots & \ldots\ldots & \\
u^{r-1}, & \sigma^{-1}u^{r-1}\sigma, & \sigma^{-2}u^{r-1}\sigma^2, & \ldots . \sigma u^{r-1}\sigma^{-1}. &
\end{array}$$

For these operations are all different, since

$$\sigma^{-i}u^{\lambda}\sigma^{i} = \sigma^{-j}u^{\mu}\sigma^{j}$$

would require $$\sigma^{-(i-j)}u^{\lambda}\sigma^{i-j} = u^{\mu},$$

where μ must be $= \lambda$. But then, a power of σ being commutative with u, either s or t would be commutative with u, which is excluded.

This group δ_4 is therefore an analogue of the not cyclical type of order pq. It exists only if r is a divisor of both $p - 1$ and $q - 1$. Its identities are

$$st = ts, \quad u^{-1}su = s^{\mu}, \quad u^{-1}tu = t^{\nu}.$$

It contains

1 self-conjugate subgroup of order p, $\{s\}$;
1 self-conjugate subgroup of order q, $\{t\}$;
pq conjugate subgroups of order r, $\{(st)^{\alpha}u\,(st)^{\alpha}\}$, $(\alpha = 0, 1, 2, \ldots. pq - 1)$;
1 self-conjugate cyclical subgroup of order pq, $\{st\}$;
q conjugate not cyclical subgroups of order pr, $\{s, t^{-\alpha}ut^{\alpha}\}$;
p conjugate not cyclical subgroups of order qr, $\{t, s^{-\alpha}us^{\alpha}\}$.

Its operations are distributed according to their orders as follows :

Order ..	1	p	q	r	pq
Number.	1	$p - 1$	$q - 1$	$pq(r - 1)$	$(p - 1)(q - 1)$

A substitution group of this type of order 30 is generated by

$s = (1, 2, 3, 4, 5)(6, 7, 8, 9, 10)(11, 12, 13, 14, 15)$
$(16, 17, 18, 19, 20)(21, 22, 23, 24, 25)(26, 27, 28, 29, 30)$.
$t = (1, 6, 11)(2, 7, 12)(3, 8, 13)(4, 9, 14)(5, 10, 15)$
$(16, 21, 26)(17, 22, 27)(18, 23, 28)(19, 24, 29)(20, 25, 30)$.
$u = (1, 16)(2, 20)(3, 19)(4, 18)(5, 17)$
$(6, 26)(7, 30)(8, 29)(9, 28)(10, 27)$
$(11, 21)(12, 25)(13, 24)(14, 23)(15, 22)$.

B.—*The subgroup H not cyclical*; $t^{-1}st = s^{\mu}$, $(\mu \neq 1)$.

This is possible only if q is a divisor of $p - 1$. The group H now contains one subgroup of order p, and p subgroups of order q. Any operation u of order

r must transform at least one of these q subgroups, say $\{t\}$, into itself. We have then, as under A,

$$u^{-1}su = s^{\nu}, \quad u^{-1}tu = t^{\rho}.$$

It follows that

$$u^{-1}(t^{-1}st)\,u = u^{-1}(s^{\mu})\,u = s^{\mu\nu}.$$

But, on the other hand,

$$\begin{aligned} u^{-1}(t^{-1}st)\,u &= u^{-1}t^{-1}u\,.\,u^{-1}su\,.\,u^{-1}tu \\ &= t^{-\rho}.\,s^{\nu}.\,t^{\rho} \\ &= s^{\mu^{\rho}\nu}. \end{aligned}$$

Hence we must have

$$\begin{aligned} \mu^{\rho}\nu &\equiv \mu\nu \pmod{p}, \\ \mu^{\rho-1} &\equiv 1 \pmod{p}. \end{aligned}$$

But since $\rho - 1 < q$ and $\mu \neq 1$, this is only possible if

$$\rho = 1.$$

We have therefore

$$u^{-1}su = s^{\nu}, \quad u^{-1}tu = t,$$

and there are two cases to be distinguished according as 5) $\nu = 1$ or 6) $\nu \neq 1$.

5). Here t and u generate a cyclical group of order qr which s transforms into p distinct conjugate groups of this order. These groups have the powers of u in common; beside these they contain $p\,(qr - r)$ distinct operations, which with the powers of su make up the entire group. It is readily seen that this group is of essentially the same form as 2) and 3) under A, the operations u, s, t here playing the same role as s, t, u in 2).

6). In this case r as well as q must be a divisor of $p - 1$. As in 5), the operations t and u generate a cyclical group of order qr which s transforms into p conjugate groups of this order. But in the present case these groups have no operation, except identity, in common. They contain therefore $p\,(qr - 1)$ distinct operations, which with the powers of s make up the entire group.

This group δ_5 exists only if q and r are both divisors of $p - 1$. Its identities are

$$t^{-1}st = s^{\mu}, \quad u^{-1}su = s^{\nu}, \quad u^{-1}tu = t.$$

It contains

1 self-conjugate subgroup of order p, $\{s\}$;
p conjugate subgroups of order q, $\{s^{-\alpha}ts^{\alpha}\}$, $(\alpha = 0, 1, \ldots. p - 1)$;
p conjugate subgroups of order r, $\{s^{-\alpha}us^{\alpha}\}$, $(\alpha = 0, 1, \ldots. p - 1)$;

1 self-conjugate not cyclical subgroup of order pq, $\{s, t\}$;
1 self-conjugate not cyclical subgroup of order pr, $\{s, u\}$;
p conjugate cyclical subgroups of order qr, $\{s^{-a}ts^{a}, u\}$, $(\alpha = 0, 1, \ldots . p - 1)$.

Its operations are distributed according to their orders as follows:

Order...	1	p	q	r	qr
Number.	1	$p-1$	$p(q-1)$	$p(r-1)$	$p(q-1)(r-1)$

A substitution group of this type of order 42 is generated by

$s = (1, 2, 3, 4, 5, 6, 7)(8, 9, 10, 11, 12, 13, 14)$
$(15, 16, 17, 18, 19, 20, 21)(22, 23, 24, 25, 26, 27, 28)$
$(29, 30, 31, 32, 33, 34, 35)(36, 37, 38, 39, 40, 41, 42)$.
$t = (1, 8, 15)(2, 10, 19)(3, 12, 16)(4, 14, 20)(5, 9, 17)$
$(6, 11, 21)(7, 13, 18)(22, 29, 36)(23, 31, 40)(24, 33, 37)$
$(25, 35, 41)(26, 30, 38)(27, 32, 42)(28, 34, 39)$.
$u = (1, 22)(2, 28)(3, 27)(4, 26)(5, 25)(6, 24)(7, 23)$
$(8, 29)(9, 35)(10, 34)(11, 33)(12, 32)(13, 31)(14, 30)$
$(15, 36)(16, 42)(17, 41)(18, 40)(19, 39)(20, 38)(21, 37)$.

ANN ARBOR, *Sept.*, 1892.